

AMENDMENTS TO THE CLAIMS

1-33. (canceled)

34. (Currently amended) An image processing system comprising:

an image providing apparatus which defines a location information indicating a plurality of regions in an image file for embedding a digital watermark in a ~~part of a region in an image file~~desired region among the plurality of regions and ~~provides~~providing said image file, in which said digital watermark is embedded based on said location information; and

an image utilizing apparatus which extracts said digital watermark from said image file provided by said image providing apparatus based on said location information, and verifies whether a data in said ~~part of a~~desired region, in which said digital watermark is embedded, has been tampered.

35. (Currently amended) An image processing system comprising:

an image providing apparatus which recognizes a format ~~of~~ for indicating a plurality of regions in an image file and provides said image file in which a digital watermark is embedded in a ~~part of a~~desired region among the plurality of regions based on said format; and

an image utilizing apparatus which recognizes said format of said image file, extracts said digital watermark from said ~~part of a~~desired region based on said format, and verifies whether a data in said ~~part of a~~desired region in said image file, in which said digital watermark is embedded, has been tampered.

36. (Original) An image processing system as claimed in claim 34 or 35, wherein said image providing apparatus provides said image file in which a different kind of said digital watermark is embedded in a different region in said image file.

37. (Original) An image processing system as claimed in claim 36, wherein said image providing apparatus provides said image file in which a different kind of said digital watermark is embedded according to an image quality in each region where said digital watermark is embedded.

38. (Original) An image processing system as claimed in claim 34, wherein:
said location information for embedding a digital watermark includes a location information of a region for displaying a specific information necessary for detecting a tamper; and
said image utilizing apparatus extracts said digital watermark with said message digest from said image file based on said location information, and generates a corresponding message digest using said specific information in said provided image file, and detects tampering with said image file by comparing said extracted message digest with said corresponding generated message digest.
39. (Original) An image processing system as claimed in claim 34, wherein:
said location information for embedding a digital watermark includes a location information of a region for displaying a specific information necessary for detecting a tamper and a location information of a region for embedding a message digest corresponding to said specific information; and
said image utilizing apparatus extracts said digital watermark with said message digest from said image file based on said location information, generates a corresponding message digest using said specific information in said provided image file, and detects tampering with said image file by comparing said extracted message digest with said corresponding generated message digest.
40. (Original) An image processing system as claimed in claim 39, wherein said region for embedding said message digest corresponding to said specific information is independent of said region for displaying said specific information necessary for detecting said tamper.
41. (Original) An image processing system as claimed in claim 34, wherein:
said location information is registered in both of said image providing apparatus and said image utilizing apparatus;
said image providing apparatus embeds said digital watermark in said image file based on said registered location information; and

said image utilizing apparatus extracts said digital watermark from said image file based on said registered location information.

42. (Original) An image processing system as claimed in claim 34, wherein:

said image providing apparatus transfers said location information to said image utilizing apparatus;

said image providing apparatus embeds said digital watermark in said image file based on said location information to be transferred; and

said image utilizing apparatus extracts said digital watermark from said image file based on said location information transferred from said image providing apparatus.

43. (Currently amended) An image providing apparatus comprising:

a location defining means which defines a location information indicating a plurality of regions in a image file for embedding a digital watermark in a ~~part of a~~desired region among the plurality of regions in an said image file; and

a providing means which provides said image file in which said digital watermark is embedded based on said location information.

44. (Currently amended) An image providing apparatus comprising:

a format recognizing means which recognizes a format ~~of~~for indicating a plurality of regions in an image file; and

a providing means which provides said image file in which a digital watermark is embedded in a ~~part of a~~desired region among the plurality of regions based on said format.

45. (Original) An image providing apparatus as claimed in claim 43 or 44,

wherein said providing means provides said image file in which a different kind of said digital watermark is embedded in a different region in said image file.

46. (Original) An image providing apparatus as claimed in claim 45, wherein said providing means provides said image file in which a different kind of said digital watermark is embedded according to an image quality in each region where said digital watermark is embedded.

47. (Original) An image providing apparatus as claimed in claim 43, wherein said location information for embedding a digital watermark includes a location information of a region for displaying a specific information necessary for detecting a tamper and a location information of a region for embedding a message digest corresponding to said specific information.

48. (Original) An image providing apparatus as claimed in claim 47, wherein said region for embedding said message digest corresponding to said specific information is independent of said region for displaying said specific information necessary for detecting said tamper.

49. (Currently amended) An image utilizing apparatus comprising:

an inputting means which inputs an image file in which a location information ~~is defined~~ indicates a plurality of regions in said image file for embedding a digital watermark in a ~~part of~~ desired region among the plurality of regions in said image file;

an extracting means which extracts said digital watermark from said image file based on said location information; and

a verifying means which verifies whether a data in said ~~part of a~~ desired region, in which said digital watermark is embedded, has been tampered.

50. (Currently amended) An image utilizing apparatus comprising:

an inputting means which inputs an image file;

a format recognizing means which recognizes said format of said image file, said format indicating a plurality of regions in said image file for embedding a digital watermark in a desired region among the plurality of regions;

an extracting means which extracts said digital watermark from ~~said part of a~~ said desired region based on said format; and

a verifying means which verifies whether a data in said ~~part of a~~desired region, in which said digital watermark is embedded, has been tampered.

51. (Original) An image utilizing apparatus as claimed in claim 49, further comprising a generating means which generates a corresponding message digest using said specific information in said input image file, and wherein:

said extracting means which extracts said digital watermark with said message digest from said image file based on said location information; and

said verifying means which detects tampering with said image file by comparing said extracted message digest with said corresponding generated message digest.

52. (Currently amended) A recording medium storing a program to be executed by a computer, said program comprising:

a location defining module which defines a location information indicating a plurality of regions in an image file for embedding a digital watermark in a ~~part of a~~desired region among the plurality of regions in an said image file; and

a providing module which provides said image file in which said digital watermark is embedded based on said location information.

53. (Currently amended) A recording medium storing a program to be executed by a computer, said program comprising:

a format recognizing module which recognizes a format ~~of~~indicating a plurality of regions in an image file; and

a providing module which provides said image file in which a digital watermark is embedded in a ~~part of a~~desired region among the plurality of regions based on said format.

54. (Original) A recording medium as claimed in claim 52 or 53, wherein said providing module provides said image file in which a different kind of said digital watermark is embedded in a different region in said image file.

55. (Original) A recording medium as claimed in claim 54, wherein said providing module provides said image file in which a different kind of said digital watermark is embedded according to an image quality in each region where said digital watermark is embedded.

56. (Original) A recording medium as claimed in claim 52, wherein said location information for embedding a digital watermark includes a location information of a region for displaying a specific information necessary for detecting a tamper and a location information of a region for embedding a message digest corresponding to said specific information.

57. (Original) A recording medium as claimed in claim 56, wherein said region for embedding said message digest corresponding to said specific information is independent of said region for displaying said specific information necessary for detecting said tamper.

58. (Currently amended) A recording medium storing a program to be executed by a computer, said program comprising:

an inputting module which inputs an image file in which a location information is ~~defined~~indicates a plurality of regions in said image file for embedding a digital watermark in a ~~part of~~desired region among the plurality of regions in said image file;

an extracting module which extracts said digital watermark from said image file based on said location information; and

a verifying module which verifies whether a data in said ~~part of~~desired region, in which said digital watermark is embedded, has been tampered.

59. (Currently amended) A recording medium storing a program to be executed by a computer, said program comprising:

an inputting module which inputs an image file;

a format recognizing module which recognizes said format of said image file, said format indicating a plurality of regions in said image file for embedding a digital watermark in a desired region among the plurality of regions;

an extracting module which extracts said digital watermark from said ~~part of a~~ desired region based on said format; and

a verifying module which verifies whether a data in said ~~part of a~~ desired region, in which said digital watermark is embedded, has been tampered.

60. (Original) A recording medium as claimed in claim 58, further comprising a generating module which generates a corresponding message digest using said specific information in said input image file, and wherein:

said extracting module which extracts said digital watermark with said message digest from said image file based on said location information; and

said verifying module which detects tampering with said image file by comparing said extracted message digest with said corresponding generated message digest.

61. (Currently amended) An image verifying method comprising:

inputting an image file in which a location information ~~is defined~~ indicates a plurality of regions in said image file for embedding a digital watermark in a ~~part of a~~ desired region among said plurality of regions in said image file;

extracting said digital watermark from said image file based on said location information;
and

verifying whether a data in said ~~part of a~~ desired region, in which said digital watermark is embedded, has been tampered.

62. (Currently amended) An image verifying method comprising:

inputting an image file;

recognizing said format of said image file, said format indicating a plurality of regions in said image file for embedding a digital watermark in a desired region among the plurality of regions;

extracting said digital watermark from said ~~part of a~~ desired region based on said format;
and

verifying whether a data in said ~~part of a~~ desired region, in which said digital watermark is embedded, has been tampered.

63. (Original) An image verifying method as claimed in claim 61, further comprising generating a corresponding message digest using said specific information in said input image file, and wherein:

said extracting said digital watermark extracts said digital watermark with said message digest from said image file based on said location information; and

said verifying tampering detects tampering with said image file by comparing said extracted message digest with said corresponding generated message digest.

64. (New) An image processing system comprising:

an image providing apparatus which provides an image file, from which a digital watermark information can be extracted by using a watermark key that includes an authentication information which authenticates said image file provided by an valid provider, and said watermark key of said image file; and

an image utilizing apparatus which extracts said digital watermark information from said image file provided by said image providing apparatus using said watermark key provided by said image providing apparatus, verifies whether said watermark key has been tampered or not using said authentication information in said watermark key, verifies whether said image file has been tampered or not using said verified watermark key, and displays said verified image file, wherein

said image providing apparatus defines a location information indicating a plurality of regions in said image file for embedding said digital watermark in a desired region among the

plurality of regions in said image file, and provides said image file in which said digital watermark is embedded based on said location information, and

said image utilizing apparatus extracts said digital watermark from said image file provided by said image providing apparatus based on said location information, and verifies whether a data in said desired region, in which said digital watermark is embedded, has been tampered.

65. (New) An image processing system comprising:

an image providing apparatus which provides an image file, from which a digital watermark information can be extracted by using a watermark key that includes an authentication information which authenticates said image file provided by an valid provider, and said watermark key of said image file; and

an image utilizing apparatus which extracts said digital watermark information from said image file provided by said image providing apparatus using said watermark key provided by said image providing apparatus, verifies whether said watermark key has been tampered or not using said authentication information in said watermark key, verifies whether said image file has been tampered or not using said verified watermark key, and displays said verified image file, wherein

said image providing apparatus recognizes a format of said image file, and provides said image file in which said digital watermark is embedded in a desired region among a plurality of regions in said image file based on said format, and

said image utilizing apparatus recognizes said format of said image file provided by said image providing apparatus, extracts said digital watermark from said desired region based on said format, and verified whether a data in said desired region, in which said digital watermark is embedded, has been tampered.

66. (New) The image processing system according to claim 34, wherein a density of said digital watermark is adjusted to a quality of said image file.

67. (New) The image processing system according to claim 66, wherein a data amount of said digital watermark for a character is smaller than one for another type of information in said image file.
68. (New) The image processing system according to claim 35, wherein a density of said digital watermark is adjusted to a quality of said image file.
69. (New) The image processing system according to claim 68, wherein a data amount of said digital watermark for a character is smaller than one for another type of information in said image file.
70. (New) The image providing apparatus according to claim 43, wherein a density of said digital watermark is adjusted to a quality of said image file.
71. (New) The image providing apparatus according to claim 70, wherein a data amount of said digital watermark for a character is smaller than one for another type of information in said image file.
72. (New) The image providing apparatus according to claim 44, wherein a density of said digital watermark is adjusted to a quality of said image file.
73. (New) The image providing apparatus according to claim 72, wherein a data amount of said digital watermark for a character is smaller than one for another type of information in said image file.
74. (New) The image utilizing apparatus according to claim 49, wherein a density of said digital watermark is adjusted to a quality of said image file.

75. (New) The image utilizing apparatus according to claim 74, wherein a data amount of said digital watermark for a character is smaller than one for another type of information in said image file.
76. (New) The image providing apparatus according to claim 50, wherein a density of said digital watermark is adjusted to a quality of said image file.
77. (New) The image providing apparatus according to claim 76, wherein a data amount of said digital watermark for a character is smaller than one for another type of information in said image file.
78. (New) The recording medium according to claim 52, wherein a density of said digital watermark is adjusted to a quality of said image file.
79. (New) The recording medium according to claim 78, wherein a data amount of said digital watermark for a character is smaller than one for another type of information in said image file.
80. (New) The recording medium according to claim 53, wherein a density of said digital watermark is adjusted to a quality of said image file.
81. (New) The recording medium according to claim 80, wherein a data amount of said digital watermark for a character is smaller than one for another type of information in said image file.
82. (New) The recording medium according to claim 58, wherein a density of said digital watermark is adjusted to a quality of said image file.

83. (New) The recording medium according to claim 82, wherein a data amount of said digital watermark for a character is smaller than one for another type of information in said image file.
84. (New) The recording medium according to claim 59, wherein a density of said digital watermark is adjusted to a quality of said image file.
85. (New) The recording medium according to claim 84, wherein a data amount of said digital watermark for a character is smaller than one for another type of information in said image file.
86. (New) The image verifying method according to claim 61, wherein a density of said digital watermark is adjusted to a quality of said image file.
87. (New) The image verifying method according to claim 86, wherein a data amount of said digital watermark for a character is smaller than one for another type of information in said image file.
88. (New) The image verifying method according to claim 62, wherein a density of said digital watermark is adjusted to a quality of said image file.
89. (New) The image verifying method according to claim 88, wherein a data amount of said digital watermark for a character is smaller than one for another type of information in said image file.
90. (New) The image processing system according to claim 64, wherein a density of said digital watermark is adjusted to a quality of said image file.

91. (New) The image processing according to claim 90, wherein a data amount of said digital watermark for a character is smaller than one for another type of information in said image file.

92. (New) The image processing system according to claim 65, wherein a density of said digital watermark is adjusted to a quality of said image file.

93. (New) The image processing according to claim 92, wherein a data amount of said digital watermark for a character is smaller than one for another type of information in said image file.